CITY OF SANDY OAKS, TEXAS

ORDINANCE NO. 2017-74

AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF SANDY OAKS, TEXAS ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM; SETTING DEFINITIONS, POLICIES AND PROCEDURES FOR IMPLEMENTATION OF THE IDENTITY THEFT PREVENTION PROGRAM; PROVIDING A SEVERABILITY CLAUSE; AND PROVIDING AN EFFECTIVE DATE.

WHEREAS, the Federal Trade Commission adopted rules pertaining to an Identity Theft Prevention Program pursuant to the Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 which requires that creditors adopt an Identity Theft Prevention Program on or before November 1, 2008; and

WHEREAS, the Red Flags Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors" and the City Council finds the City is therefore classified as a creditor; and

WHEREAS, the City Council has reviewed the Identity Theft Prevention Program attached hereto as Exhibit A and believes it fulfills, complies and implements the Red Flags Rule and other requirements outlined by the Federal Trade Commission; and

WHEREAS, the City of Sandy Oaks, Texas ("City") has determined that the following Identity Theft Prevention Program is in the best interest of the City and its citizens;

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF SANDY OAKS, TEXAS:

Section 1. Findings. The foregoing recitals are hereby found to be true and correct and are hereby adopted by the City Council and made a part hereof for all purposes as findings of fact.

Section 2. Adoption of Identity Theft Prevention Program. The City Council hereby adopts the Identity Theft Prevention Program ("Program") as is more particularly set out in Exhibit A attached hereto and incorporated herein.

Section 3. Implementation. All procedures and requirements of the Program shall be implemented as outlined in Exhibit A.

Section 4. Severability. Should any sentence, paragraph, subdivision, clause, phrase or section of the Ordinance be adjudged or held to be unconstitutional, illegal or invalid, the same shall not affect the validity of this Ordinance as a whole, or any part or provision thereof other than the part so decided to be invalid, illegal or unconstitutional, and shall not affect the validity of this Ordinance as a whole.

Section 5. Effective Date. This Ordinance shall take effect immediately from and after its passage.

PASSED, ADOPTED and **APPROVED** this 8th day of June, 2017.

CITY OF SANDY OAKS, TEXAS

Karen Tanguma
Karen Mendiola Tanguma, Mayor

ATTEST:

Charlotte Rabe
Charlotte Rabe, City Clerk

CITY OF SANDY OAKS, TEXAS
IDENTITY THEFT PREVENTION PROGRAM

SECTION 1. BACKGROUND. The risk to the City of Sandy Oaks ("City"), its employees and customers from data loss and identity theft is of significant concern to the City and can be reduced only through the combined efforts of every employee and contractor. The City Council therefore adopts this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule") which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), 16 C.F.R. 681.2. The City Council approved the Program on March 9, 2017.

SECTION 2. PURPOSE AND DEFINITIONS.

A. Establish an Identity Theft Prevention Program. The City Council establishes this Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Section 114 of FACTA.

B. Establishing and Fulfilling Requirements of the Red Flags Rule.

1. The Rule defines "identity theft" as "fraud committed using the identifying information of another person" and a "red flag" as a pattern, practice or specific activity that indicates the possible existence of Identity theft.

2. Under the Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. The Program must contain reasonable policies and procedures to:

    a. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the Program;
    b. Detect red flags that have been incorporated into the Program;
    c. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
    d. Ensure the Program is updated periodically, to reflect changes in risks to customers or to safety and soundness of the creditor from identity theft.

C. Implementation of Program. This Program enables the City to protect existing customers, reducing risk from identity fraud, and minimize potential damage to the City from fraudulent new accounts. The Program will help the City:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;

2. Detect risks when they occur in covered accounts;

3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and

4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the Program.

D. Definitions used in this Program.

1. City -- The City of Sandy Oaks, Texas.

2. Covered Account -- Any account the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions and any other account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from identity theft.

3. Creditors – Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors.

4. Identifying information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's International Protocol address or routing code.

5. Program: The Identity Theft Prevention Program for the City.

6. Program Administrator: The City Administrator is the Program Administrator of the Program. In the event the City Administrator's position is vacant, the Mayor will act as Program Administrator.

SECTION 3. IDENTIFICATION OF RED FLAGS. In order to identify relevant red flags, the City considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, and the methods it provides to access its accounts. The following are potential for fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification. The City identifies the following red flags in each of the listed categories.

A. Notifications and Warnings for Consumer Credit Reporting Agencies

1. Alerts, notifications or warnings from a consumer reporting agency;

2. A fraud or active duty alert included with a consumer report;

3. A notice of a credit freeze from a consumer reporting agency in response to a request for a consumer report; or

4. A notice of address discrepancy from a consumer reporting agency as defined in 334.82(b) of the FACTA.

5. Consumer reports that indicate a pattern of activity with the history and usual pattern of activity of an applicant or customer, such as:

    a. A recent and significant increase in volume of inquires;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. Suspicious documents.

1. Documents provided for identification that appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

3. Other information on the identification is not consistent with information provided by the person opening the new covered account or customer presenting the identification.

4. Other information in the identification is not consistent with readily accessible information that is on file with the City, such as signature card or a recent check.

5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious personal identifying information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the City. For example:

    a. The address does not match any address in the consumer report;
    b. The social security number has not been issued or is listed on the Social Security Administration's Death Master File; or
    c. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the

customer. For example, there is a lack of correlation between the social security number range and date of birth.

2. Personal identifying information provided is associated with known fraudulent activity as indicated by external or third-party sources used by the City. For example, the address on the application is the same as the address provided on the fraudulent application.

3. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the City. For example:

    a. The address on the application is fictitious, a mail drop, or a prison; or
    b. The phone number is invalid or is associated with a pager or answering service.

4. The social security number provided is the same as that submitted by other persons opening an account or other customers.

5. The address or telephone number provided is the same as or like the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.

6. The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is complete.

7. Personal identifying information provided is inconsistent with personal identifying information that is on file with the City.

8. When using security question (mother's maiden name, pet's name, etc.) the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. Unusual use of, or suspicious activity related to, the covered account.

1. Shortly following the notice of a change of address for a covered account, the City receives a request for new, additional, or replacement of goods or services, of for the addition of authorized users on the account.

2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but to subsequent payments.

3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;
b. A material change in purchasing or usage patterns.

4. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

6. The City is notified that the customer is not receiving paper account statements.

7. The City is notified of unauthorized charges or transactions in connection with the customer's covered account.

8. The City receives notice from customers, victims of identity theft, law enforcement authorities, or other reasons regarding possible identity theft in connection with he covered accounts held by the City.

9. The City is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

E. Alerts from others. Notice to the City from a customer, identity theft victim, fraud detection service, law enforcement or other persons that it has opened or is maintained a fraudulent account for a person engaged in identity theft.

SECTION 4. DETECTING RED FLAGS.

A. New Accounts. In order to detect any of the red flags identified above associated with the opening of a new account, City personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity;
4. Request additional documentation to establish identity; and
5. Independently contact the customer or business.

B. Existing Accounts. In order to detect any of the red flags identified above for an existing account, City personnel will take the following steps to monitor transactions with an account:

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, or via email);
2. Verify the validity of requests to close accounts or change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

SECTION 5. RESPONDING TO RED FLAGS.

A. Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the City from damages and loss.

1. Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present the information to the designated authority for determination.

2. The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

B. If the transaction is determined to be fraudulent, appropriate action must be taken immediately. Actions may include:

1. Cancelling the transaction;

2. Notifying and cooperating with law enforcement;

3. Determining the extent of liability of the City; and

4. Notifying the actual customer that fraud has been attempted.

SECTION 6. PREVENTING AND MITIGATING IDENTITY THEFT. In the event City personnel detect any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the red flag:

A. Prevent and Mitigate.

1. Continue to monitor an account for evidence of identity theft;

2. Contact the customer, sometimes through multiple methods;

3. Change any passwords or other security devices that permit access to accounts;

4. Not open a new account;

5. Close an existing account;

6. Do not close the account, but monitor or contact authorities;

7. Reopen an account with a new number;

8. Notify the Program Administrator for determination of the appropriate step(s) to take;

9. Notify law enforcement; or

10. Determine that no response is warranted under the particular circumstances.

B. Protect customer-identifying information. In order to further prevent the likelihood of identity theft occurring with respect to City accounts, the City will take the following steps with respect to its internal operating procedures to protect customer-identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;

2. Where and when allowed, ensure complete and secure destruction of paper documents and computer files containing customer information;

3. Ensure that office computers are password protected and that computer screens lock after a set period of time;

4. Change passwords on office computers on a regular basis;

5. Ensure all computers are backed up properly and any backup information is secured;

6. Keep offices clear of papers containing customer information;

7. Request on the last 4 digits of the social security number (if any);

8. Ensure computer virus protection is up to date; and

9. Require and keep only the kinds of customer information that are necessary for City account purposes.

SECTION 7. PERIODIC UPDATES TO PROGRAM.

A. At periodic intervals established in the Program, or as required, the Program will be reevaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment.

B. Periodic reviews will include an assessment of which accounts are covered by the Program.

C. As part of the review, red flags may be revised, replaced, or eliminated. Defining new red flags may also be appropriate.

D. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the City and its customers.

SECTION 8. PROGRAM ADMINISTRATION.

A. Involvement of Management.

1. The Program is the responsibility of the City Council. Approval of the initial plan must be appropriately documented and maintained.

2. Operational responsibility of the program is delegated to the City Administrator.

B. Staff Training.

1. Staff training shall be conducted for all employees, officials, and contractors when it is reasonably foreseeable that they may come in contact with accounts or personally identifiable information that may constitute a risk to the City or its customers.

2. The City Administrator is responsible for ensuring identity theft training for all requisite employees and contractors.

3. Employees must receive annual training in all elements of the Program.

4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the Program are made.

C. Oversight of service providers' arrangements

1. It is the responsibility of the City to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Rule and validated by appropriate due diligence, may be considered to be meeting the requirement.

3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

D. Specific Program Elements and Confidentiality. For the effectiveness of identity theft Prevention Programs, the Rule envisions a degree of confidentiality regarding the City's specific practices relating to identity theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices are to be limited to those employees who need to know them for purposes of preventing identity theft. Because this Program is to be adopted by a public body and thus publicly available, it is counterproductive to list the specific practices here. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed in this document.